

4



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/939,810	08/28/2001	Jinglong F. Zhang		2927

7590 07/12/2005  
Jinglong Frank Zhang  
10909 Santa Clara Dr.  
Fairfax, VA 22030

EXAMINER

ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/939,810

Applicant(s)

ZHANG, JINGLONG F.

Examiner

Kaveh Abrishamkar

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 28 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>8/28/2001</u> .   | 6) <input type="checkbox"/> Other: _____                                    |

10

### **DETAILED ACTION**

1. This action is in response to the communication filed on August 28, 2001. Claims 1-20 were originally received for consideration. No preliminary amendments regarding the claims were received. Claims 1-20 are currently being considered.

#### ***Information Disclosure Statement***

2. An initialed and dated copy of the Applicant's IDS form 1449, received on August 28, 2001, is attached to this Office action.

#### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1,3,5,6,9,10,11,15,16,17,18, and 20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.
4. Claim 1 discloses the terms "encryptor," "message," and "decryptor." These terms are not disclosed in the specification, and it is unclear what the encryptor and

decryptor encompass, how the system of the encryption/decryption is set-up, and what sort of message is being transmitted.

5. Claim 1 discloses the relationship " $b(f(m))=m$ ." This relationship is not disclosed in the specification.

6. Claim 3 discloses the terms "encryptor," "message," and "decryptor." These terms are not disclosed in the specification, and it is unclear what the encryptor and decryptor encompass, how the system of the encryption/decryption is set-up, and what sort of message is being transmitted.

7. Claim 5 discloses "mapping." There is no mention of any mapping function in the specification, and therefore, it is unclear what sort of mapping is being performed.

8. Claim 5 discloses "transforming X to Y" and "W to U." However, this transformation is not disclosed in the specification and therefore, it is not clear what transformation functions are being used.

9. Claim 5 discloses "satisfying  $x_{sub.i} > \beta_{sub.1}x_{sub.1} + \beta_{sub.2}x_{sub.2} + \dots + \beta_{sub.i-1}x_{sub.i-1} + \gamma_{sub.1}w_{sub.1} + \gamma_{sub.2}w_{sub.2} + \dots + \gamma_{sub.i}w_{sub.i}$  where, for  $1 \leq i \leq n$ ,  $\gamma_{sub.i} = f_{sub.i}(\beta_{sub.i})$  and  $\beta_{sub.i} \in \text{elect cons.}[0, 2^{sup.h})$ ." This relationship is not defined in the specification, and therefore, it is unclear what beta represents.

10. Claim 5 discloses the variable "S." There is no definition of "S" in the specification, so it is unclear what "S" represents.

11. Claim 6 discloses the terms "encryptor" and "decryptor." These terms are not disclosed in the specification, and it is unclear what the encryptor and decryptor encompass, and how the system of the encryption/decryption is set-up.

12. Claim 9 discloses "chaining." However, no sort of "chaining" is described in the specification, and therefore, it is unclear what is function "chaining" actually performs.

13. Claim 10 discloses "a set of mapping functions." There is no mention of any mapping function in the specification, and therefore, it is unclear what sort of mapping is being performed.

14. Claim 11 discloses the relationship " $b_i(f(m)) \neq b_j(f(m))$ ." This relationship is not disclosed in the specification.

15. Claim 15 discloses the terms "encryptor," "message," and "decryptor." These terms are not disclosed in the specification, and it is unclear what the encryptor and decryptor encompass, how the system of the encryption/decryption is set-up, and what sort of message is being transmitted.

16. Claim 16 discloses the terms "encryptor," "message," and "decryptor." These terms are not disclosed in the specification, and it is unclear what the encryptor and decryptor encompass, how the system of the encryption/decryption is set-up, and what sort of message is being transmitted.

17. Claim 17 discloses "mapping." There is no mention of any mapping function in the specification, and therefore, it is unclear what sort of mapping is being performed.

Art Unit: 2131

18. Claim 17 discloses "transforming X to Y" and "W to U." However, this transformation is not disclosed in the specification and therefore, it is not clear what transformation functions are being used.

19. Claim 17 discloses "satisfying  $x_{i-1} > \beta_1 x_1 + \beta_2 x_2 + \dots + \beta_{i-1} x_{i-1} + \gamma_1 w_1 + \gamma_2 w_2 + \dots + \gamma_i w_i$  where, for  $1 \leq i \leq n$ ,  $\gamma_i = f_i(\beta_i)$  and  $\beta_i \in [0, 2^h]$ ." This relationship is not defined in the specification, and therefore, it is unclear what  $\beta$  represents.

20. Claim 17 discloses the variable "S." There is no definition of "S" in the specification, so it is unclear what "S" represents.

21. Claim 18 discloses the terms "encryptor" and "decryptor." These terms are not disclosed in the specification, and it is unclear what the encryptor and decryptor encompass, and how the system of the encryption/decryption is set-up.

22. Claim 19 discloses "additions." However, there is no mention of this operation in the specification, and the purpose of the addition is unclear based on the specification.

23. Claim 20 discloses "a message." It is unclear what sort of message is being transmitted based on the specification.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

24. Claim 19 recites the limitation "said additions" in the third line of the claim. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

25. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Kurumatani (U.S. Patent No. 6,876,745).

Regarding claim 1, Kurumatani discloses:

A cryptographic method, where a non-empty set  $F$  of encryption keys  $F_{\text{sub.1}}$ ,  $F_{\text{sub.2}}$ ,  $F_{\text{sub.3}}$ , . . . are associated with one single decryption key  $B$  satisfying  $b(f(m))=m$  for any input  $m$  and for  $b$  being a decryption function employing  $B$  and for  $f$  being an encryption function employing any  $F_{\text{sub.i}}$ ,  $i \in \text{cons. } F$ , comprising:

obtaining arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

generating a decryption key; generating one of a plurality of corresponding encryption keys (column 8 lines 39-64);

supplying an encryptor with said encryption key (column 9 lines 14-17);

Art Unit: 2131

accepting a message m (column 9 lines 14-17);  
encrypting m by said encryptor to ciphertext c using said encryption key (column 9 lines 14-17);  
supplying a decryptor with said decryption key (column 9 lines 17-22); and  
decrypting c by said decryptor to recover m using said decryption key (column 9 lines 17-22).

Regarding claim 2, Kurumatani discloses:

A cryptographic method for establishing a secret between two parties comprising:  
generating a secrecy primitive (column 8 line 38 – column 9 line 29); and  
establishing said secret between said two parties using said secrecy primitive (column 8 line 38 – column 9 line 29).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 1 comprising:  
obtaining arbitrary and/or random input from which cryptographic keys are generated;  
generating a decryption key (column 5 lines 53-61);  
generating a corresponding encryption key through a series of transforms where at least one of said transforms facilitates the introduction of arbitrary or random noise of any desired sufficient amount (column 4 lines 43-67, column 8 lines 39-64);

supplying an encryptor with said encryption key (column 9 lines 14-17);  
accepting a message  $m$  (column 9 lines 14-17);  
encrypting  $m$  by said encryptor to ciphertext  $c$  using said encryption key (column 9 lines 14-17);  
supplying a decryptor with said decryption key (column 9 lines 17-22); and  
decrypting  $c$  by said decryptor to recover  $m$  using said decryption key (column 9 lines 17-22).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 1 comprising:  
obtaining arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);  
generating a decryption key including a set of parameters  $p$  in normal positional number representation (column 8 lines 39-64);  
generating a corresponding encryption key comprising:  
converting  $p$  to self-contained components (column 4 lines 43-67, column 9 lines 1-22);  
constructing encryption key parameters from said self-contained components by inserting zero or more arbitrary/random components in arbitrarily or randomly chosen component positions (column 4 lines 43-67, column 9 lines 1-22); and

Art Unit: 2131

generating all other encryption key parameters (column 4 lines 43-67, column 9 lines 1-22);

supplying an encryptor with said encryption key (column 9 lines 14-17);

accepting a message  $m$  (column 9 lines 14-17);

encrypting  $m$  by said encryptor to ciphertext  $C$  using said encryption key (column 9 lines 14-17);

supplying a decryptor with said decryption key (column 9 lines 17-22); and

decrypting  $c$  by said decryptor to recover  $m$  using said decryption key (column 9 lines 17-22).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Kurumatani discloses:

A cryptographic method, as in claim 1, adopting  $n$  integer functions  $f_{\text{sub.1}}$ ,  $f_{\text{sub.2}}$ , . . . ,  $f_{\text{sub.n}}$  mapping from  $[0, 2^{\text{sup.h}})$  to  $[0, 2^{\text{sup.h}+\text{delta}})$ , where  $h > 1$  and  $2^{\text{sup.h}+\text{delta}} > 1$ , comprising:

obtaining arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

generating a decryption key, including the generation of a first set of positive integers  $X = \{x_{\text{sub.1}}, x_{\text{sub.2}}, \dots, x_{\text{sub.n}}\}$  and a second set of positive integers

$W = \{w_{\text{sub.1}}, w_{\text{sub.2}}, \dots, w_{\text{sub.n}}\}$  satisfying

$x_{\text{sub.i}} > \beta_{\text{sub.1}}x_{\text{sub.1}} + \beta_{\text{sub.2}}x_{\text{sub.2}} + \dots + \beta_{\text{sub.i-1}}x_{\text{sub.i-1}}$

$+ \gamma_{\text{sub.1}}w_{\text{sub.1}} + \gamma_{\text{sub.2}}w_{\text{sub.2}} + \dots + \gamma_{\text{sub.i}}w_{\text{sub.i}}$  where,

Art Unit: 2131

for  $1 \leq i \leq n$ ,  $\gamma_{sub.i} = f_{sub.i}(\beta_{sub.i})$  and  $\beta_{sub.i}$  di-elect cons.[0, 2<sup>sup.h</sup>) (column 8 lines 39-64);

transforming  $X$  to  $Y = \{y_{sub.1}, y_{sub.2}, \dots, y_{sub.n}\}$  and  $W$  to  $U = \{u_{sub.1}, u_{sub.2}, \dots, u_{sub.n}\}$ , including an optional permutation and one or more rounds of invertible strong modular multiplication (column 4 lines 43-67); and

further transforming  $Y$  to  $Z = \{z_{sub.1}, z_{sub.2}, \dots, z_{sub.n}\}$  and  $U$  to  $V = \{v_{sub.1}, v_{sub.2}, \dots, v_{sub.n}\}$  satisfying the following:

- a.  $p_{sub.0}, p_{sub.1}, \dots, p_{sub.t-1}$  are pairwise co-prime (column 4 lines 43-67)
- b.  $z_{sub.i} = (z_{sub.i}, 0, z_{sub.i}, 1, \dots, z_{sub.i}, qt-1)$  for  $1 \leq i \leq n$  and  $q \geq 1$  (column 4 lines 43-67)
- c.  $J = \{j_{sub.0}, j_{sub.1}, \dots, j_{sub.k-1}\}$  is a set of arbitrary or random indices where  $0 \leq j_{sub.0}, j_{sub.2}, \dots, j_{sub.k-1} < t$  (column 4 lines 43-67)
- d.  $S = \{s_{sub.0}, s_{sub.1}, \dots, s_{sub.k-1}\}$  is an arbitrary or random set satisfying:  $0 \leq s_{sub.0}, s_{sub.1}, \dots, s_{sub.k-1} < qt$ , and  $S \% t = \{s_{sub.0} \% t, s_{sub.1} \% t, \dots, s_{sub.k-1} \% t\} = J$  (column 4 lines 43-67)
- e.  $PI.p_{sub.j} \text{ di-elect cons. } J > \beta_{sub.1} y_{sub.1} + \beta_{sub.2} y_{sub.2} + \dots + \beta_{sub.n} y_{sub.n} + \gamma_{sub.1} u_{sub.1} + \gamma_{sub.2} u_{sub.2} + \dots + \gamma_{sub.n} u_{sub.n}$  (column 4 lines 43-67)
- f.  $z_{sub.i}, s_{sub.i} \text{ di-elect cons. } S = y_{sub.i} \% p_{sub.s} \% t$  (column 4 lines 43-67)
- g.  $z_{sub.i}, s_{sub.i} \text{ di-elect cons. } SS$  are arbitrary or random numbers modulo  $p_{sub.s} \% t$  for  $0 \leq s < qt$  (column 4 lines 43-67)

Art Unit: 2131

h.  $v_{sub.i} = (v_{sub.i, 0}, v_{sub.i, 1}, \dots, v_{sub.i, qt-1})$  for  $1 \leq i \leq n$  (column 4 lines 43-67)

i.  $v_{sub.i}, s_{di-elect cons.S} = w_{sub.i} \% p_{sub.s \% t}$  (column 4 lines 43-67)

j.  $v_{sub.i}, sS$  are arbitrary or random numbers modulo  $p_{sub.s \% t}$  for  $0 \leq s < qt$ .  
(column 4 lines 43-67)

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 5 further comprising:

supplying an encryptor with said encryption key (column 9 lines 14-17);

encrypting by said encryptor one or more  $n_h$ -bit data blocks which are divided into  $h$ -bit sub-blocks  $d_{sub.1}, d_{sub.2}, \dots$ , where each block is encrypted to  $c = (c_{sub.0}, c_{sub.1}, \dots, c_{sub.qt-1})$  with  $c_{sub.s} = (d_{sub.1}z_{sub.1}, s + d_{sub.2}z_{sub.2}, s + \dots + d_{sub.n}z_{sub.n}, x + f_{sub.1}(d_{sub.1})v_{sub.1}, s + f_{sub.2}(d_{sub.2})v_{sub.2}, s + \dots + f_{sub.n}(d_{sub.n})v_{sub.n}, s) \% p_{sub.s \% t}$  for  $0 \leq s < qt$  (column 9 lines 14-17);

supplying a decryptor with said decryption key (column 9 lines 17-22); and

decrypting by said decryptor each of said encrypted blocks  $C$  to recover said data blocks, by extracting  $C = \{c_{sub.s} \text{ vertline } s_{di-elect cons.S}\}$  from  $c$  and by repeating, for each  $d_{sub.i}$  for  $1 \leq i \leq n$ , the following:

a. converting  $C$  to a form where  $d_{sub.i}$  can be determined (column 9 lines 17-22)

b. obtaining  $d_{sub.i}$  from said converted  $C$  (column 9 lines 17-22)

Art Unit: 2131

c. removing from said converted C the quantity that d.sub.i introduced (column 9 lines 17-22).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 6, where said encryption is carried out, in lieu, independently on self-contained components, comprising:

calculating c by carrying out two or more of said additions (+) and/or by computing two or more of said terms d.sub.iz.sub.ij and f.sub.i(d.sub.i)v.sub.i, j in parallel (column 9 lines 14-17).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Kurumatani discloses:

A cryptographic method, as in claim 1, for communicating a message securely from a first party E to a second party D comprising:

obtaining at party D arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

generating at party D a decryption key to be kept secret (column 8 lines 39-64);

generating at party D one of a plurality of corresponding encryption keys (column 9 lines 1-22);

distributing said encryption key from party D to party E (column 9 lines 14-17);

accepting a message m at party E (column 9 lines 14-17);

Art Unit: 2131

encrypting  $m$  to ciphertext at party E, employing said encryption key (column 9 lines 14-17);

transmitting said ciphertext from party E to party D (column 9 lines 14-22);

receiving said ciphertext at party D (column 9 lines 14-22); and

decrypting said ciphertext at party D to recover  $m$ , employing said decryption key (column 9 lines 17-22).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 8 further comprising:

applying chaining in the encryption of  $m$  to  $c$  with zero or more blocks of arbitrary or random bits pre-pended to  $m$  (column 9 lines 14-17).

Claim 10 is rejected as applied above in rejecting claim 5. Furthermore, Kurumatani discloses:

A cryptographic method, as in claim 5, using dynamic mapping for communicating a message securely from a first party E to a second party D which generates said encryption key to be kept secret and said decryption key to be sent to party E, further comprising:

agreeing upon a set of mapping functions  $f_{\text{sub.1}}$ ,  $f_{\text{sub.2}}$ , . . . ,  $f_{\text{sub.n}}$  for said current communication by said two parties, where said set of mapping functions only

Art Unit: 2131

observe their domain and range restrictions and are independent of and unrelated to any other encryption or decryption parameters (column 4 lines 43-67);

distributing said encryption key from party D to party E (column 9 lines 14-17);

accepting a message  $m$  at party E (column 9 lines 14-17);

encrypting  $m$  to ciphertext at party E, employing said encryption key and  $f_{\text{sub.1}}$ ,  $f_{\text{sub.2}}$ , . . . ,  $f_{\text{sub.n}}$ ; transmitting said ciphertext from party E to party D over a communication channel (column 9 lines 14-17);

receiving said ciphertext at party D (column 9 lines 14-22); and

decrypting said ciphertext at party D to recover  $m$ , employing said decryption key and  $f_{\text{sub.1}}$ ,  $f_{\text{sub.2}}$ , . . . ,  $f_{\text{sub.n}}$  (column 9 lines 17-22).

Claim 11 is rejected as applied above in rejecting claim 2. Furthermore, Kurumatani discloses:

A cryptographic method, as in claim 2, where one encryption key  $F_{\text{sub.x}}$  is associated with a non-empty set  $B_{\text{sub.x}}$  of decryption keys  $B_{\text{sub.x,1}}$ ,  $B_{\text{sub.x,2}}$ , . . . ,  $B_{\text{sub.x,n}}$  satisfying  $b_{\text{sub.i}}(f(m)) \neq b_{\text{sub.j}}(f(m))$  for one or more input  $m$  if  $i \neq j$ , with  $b_{\text{sub.i}}$  and  $b_{\text{sub.j}}$  being decryption functions employing  $B_{\text{sub.x,i}}$  and  $B_{\text{sub.x,j}}$  respectively and  $f$  being an encryption function employing  $F_{\text{sub.x}}$ , comprising:

obtaining at a first party D arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

generating at party D secret decryption keys  $B_{\text{sup.1}}$ ,  $B_{\text{sup.2}}$ , . . . ,  $B_{\text{sup.k}}$  where  $B_{\text{sup.x}} \cap B_{\text{sub.x}} = \emptyset$  for  $1 \leq x \leq k$  (column 9 lines 39-64);

Art Unit: 2131

generating at party D encryption keys  $F_{sub.1}, F_{sub.2}, \dots, F_{sub.k}$  as said secrecy primitive, where  $F_{sub.x}$  corresponds to  $B_{sub.x}$  for  $1 \leq x \leq k$  (column 9 lines 1-22);

distributing said encryption keys from party D to a second party E (column 9 lines 14-17); and

establishing said secret between said two parties by making use of said encryption keys and decryption keys (column 9 lines 14-22).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Kurumatani discloses:

A cryptographic method, as in claim 11, for establishing said secret comprising:  
generating at party D said encryption keys and decryption keys (column 9 lines 14-22);

distributing said encryption keys from party D to party E (column 9 lines 14-17);

receiving said encryption keys at party E (column 9 lines 14-17);

encrypting arbitrary or random data blocks at party E employing said encryption keys (column 9 lines 14-17);

transmitting said encrypted data blocks from party E to party D over a communication channel (column 9 lines 14-22);

receiving at party D said encrypted data blocks from party E (column 9 lines 14-22);

decrypting said encrypted data blocks employing said decryption keys at party D to obtain information/characteristics about said data blocks (column 9 lines 17-22); and communicating to party E by party D, based on said information/characteristics gained about said data blocks, instructions to transform a special entity to a form from which party E learns said secret party D intends to convey and establish (column 9 lines 14-22).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 12 further comprising:  
using said established secret for further secure communications and cryptographic applications between said two parties (column 9 lines 14-22).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Kurumatani discloses:

A cryptographic method as in claim 1 for the zero-knowledge authentication/identification of a party possessing said secret decryption key comprising:

proving said authenticity/identity by said party through the exhibition of the ability to decrypt any valid encrypted messages using said decryption key (column 9 lines 17-22).

Regarding claim 15, Kurumatani discloses:

A cryptographic system, where a non-empty set  $F$  of complete encryption keys  $F_{\text{sub.1}}, F_{\text{sub.2}}, F_{\text{sub.3}}, \dots$  are associated with one single decryption key  $B$  satisfying  $b(f(m))=m$  for any input  $m$  and for  $b$  being a decryption mechanism employing  $B$  and for  $f$  being an encryption mechanism employing any  $F_{\text{sub.i}}$ , comprising:

means for obtaining arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

means for generating a decryption key (column 8 lines 39-64);

means for generating one of a plurality of corresponding encryption keys (column 9 lines 1-22);

means for supplying an encryptor with said encryption key; means for accepting a message  $m$  (column 9 lines 14-17);

means for encrypting  $m$  by said encryptor to ciphertext  $C$  using said encryption key (column 9 lines 14-17);

means for supplying a decryptor with said decryption key (column 9 lines 17-22);

and

means for decrypting  $c$  by said decryptor to recover  $m$  using said decryption key (column 9 lines 17-22).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Kurumatani discloses:

A cryptographic system as in claim 15 comprising:

means for obtaining arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

means for generating a decryption key including a set of parameters  $p$  in normal positional number representation (column 8 lines 39-64);

means for generating a corresponding encryption key comprising:

means for converting  $p$  to self-contained components (column 4 lines 43-67, column 9 lines 1-22);

means for constructing encryption key parameters from said self-contained components by inserting zero or more arbitrary/random components in arbitrarily or randomly chosen component positions (column 4 lines 43-67, column 9 lines 1-22); and

means for generating all other encryption key parameters (column 4 lines 43-67, column 9 lines 1-22);

means for supplying an encryptor with said encryption key (column 9 lines 14-17);

means for accepting a message  $m$  (column 9 lines 14-17);

means for encrypting  $m$  by said encryptor to ciphertext  $c$  using said encryption key (column 9 lines 14-17);

means for supplying a decryptor with said decryption key (column 9 lines 17-22);  
and

means for decrypting  $c$  by said decryptor to recover  $m$  using said decryption key (column 9 lines 17-22).

Claim 17 is rejected as applied above in rejecting claim 15. Furthermore, Kurumatani discloses:

A cryptographic system, as in claim 15, with means for implementing  $n$  integer functions  $f_{sub.1}, f_{sub.2}, \dots, f_{sub.n}$  mapping from  $[0, 2^{sup.h})$  to  $[0, 2^{sup.h+\delta})$ , where  $h > 1$  and  $2^{sup.h+\delta} > 1$ , comprising:

means for obtaining arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

means for generating a decryption key, including the generation of a first set of positive integers  $X = \{x_{sub.1}, x_{sub.2}, \dots, x_{sub.n}\}$  and a second set of positive integers  $W = \{w_{sub.1}, w_{sub.2}, \dots, w_{sub.n}\}$  satisfying  $x_{sub.i} > \beta_{sub.1}x_{sub.1} - \beta_{sub.2}x_{sub.2} + \dots + \beta_{sub.i-1}x_{sub.i-1} + \gamma_{sub.1}w_{sub.1} - \gamma_{sub.2}w_{sub.2} + \dots + \gamma_{sub.i}w_{sub.i}$  where, for  $1 \leq i \leq n$ ,  $\gamma_{sub.i} = f_{sub.i}(\beta_{sub.i})$  and  $\beta_{sub.i} \in \text{cons.}[0, 2^{sup.h})$  (column 9 lines 17-22);

means for transforming  $X$  to  $Y = \{y_{sub.1}, y_{sub.2}, \dots, y_{sub.n}\}$  and  $W$  to  $U = \{u_{sub.1}, u_{sub.2}, \dots, u_{sub.n}\}$ , including an optional permutation and one or more rounds of invertible strong modular multiplication (column 4 lines 43-67);

means for further transforming  $Y$  to  $Z = \{z_{sub.1}, z_{sub.2}, \dots, z_{sub.n}\}$  and  $U$  to  $V = \{v_{sub.1}, v_{sub.2}, \dots, v_{sub.n}\}$  satisfying the following:

a.  $p_{sub.0}, p_{sub.1}, \dots, p_{sub.t-1}$  are pairwise co-prime (column 4 lines 43-67)

Art Unit: 2131

b.  $z_{.i} = (z_{.i, 0}, z_{.i, 1}, \dots, z_{.i, qt-1})$  for  $1 \leq i \leq n$  and  $q \geq 1$  (column 4 lines 43-67)

c.  $J = \{j_{.0}, j_{.1}, \dots, j_{.k-1}\}$  is a set of arbitrary or random indices where  $0 \leq j_{.0}, j_{.2}, \dots, j_{.k-1} < t$  (column 4 lines 43-67)

d.  $S = \{s_{.0}, s_{.1}, \dots, s_{.k-1}\}$  is an arbitrary or random set satisfying:  
 $0 \leq s_{.0}, s_{.1}, \dots, s_{.k-1} < qt$ , and  $S \% t = \{s_{.0} \% t, s_{.1} \% t, \dots, s_{.k-1} \% t\} = J$  (column 4 lines 43-67)

e.  $Pl.p_{.j} \text{ di-elect cons. } J > .\beta_{.1} y_{.1} + .\beta_{.2} y_{.2} + \dots + .\beta_{.n} y_{.n} + .\gamma_{.1} u_{.1} + .\gamma_{.2} u_{.2} + \dots + .\gamma_{.n} u_{.n}$  (column 4 lines 43-67)

f.  $z_{.i}, s \text{ di-elect cons. } S = y_{.i} \% p_{.s} \% t$  (column 4 lines 43-67)

g.  $z_{.i}, sS$  are arbitrary or random numbers modulo  $p_{.s} \% t$  for  $0 \leq s < qt$  (column 4 lines 43-67)

h.  $v_{.i} = (v_{.i, 0}, v_{.i, 1}, \dots, v_{.i, qt-1})$  for  $1 \leq i \leq n$  (column 4 lines 43-67)

i.  $v_{.i}, s \text{ di-elect cons. } S = w_{.i} \% p_{.s} \% t$  (column 4 lines 43-67)

j.  $v_{.i}, sS$  are arbitrary or random numbers modulo  $p_{.s} \% t$  for  $0 \leq s < qt$ . (column 4 lines 43-67).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Kurumatani discloses:

A cryptographic system as in claim 17 further comprising:

Art Unit: 2131

means for supplying an encryptor with said encryption key (column 9 lines 14-17);

means for encrypting by said encryptor one or more  $nh$ -bit data blocks which are divided into  $h$ -bit sub-blocks  $d_{sub.1}, d_{sub.2}, \dots, d_{sub.n}$ , where each block is encrypted to  $c=(c_{sub.0}, c_{sub.1}, \dots, c_{sub.qt-1})$  with  $c_{sub.s}=(d_{sub.1}z_{sub.1}, s+d_{sub.2}z_{sub.2}, s+\dots+d_{sub.n}z_{sub.n}, s+f_{sub.1}(d_{sub.1})v_{sub.1}, s+f_{sub.2}(d_{sub.2})v_{sub.2}, s+\dots+f_{sub.n}(d_{sub.n})v_{sub.n}, s) \% p_{sub.s}\%$  for  $0 \leq s < qt$  (column 9 lines 14-17);

means for supplying a decryptor with said decryption key (column 9 lines 17-22);  
and

means for decrypting by said decryptor each of said encrypted blocks  $c$  to recover said data blocks, by extracting  $C=\{c_{sub.s} \text{ vertline } s \text{ di-elect cons } S\}$  from  $c$  and by repeating, for each  $d_{sub.i}$  for  $1 \leq i \leq n$ , the following:

- a. converting  $C$  to a form where  $d_{sub.i}$  can be determined (column 9 lines 17-22)
- b. obtaining  $d_{sub.i}$  from said converted  $C$  (column 9 lines 17-22)
- c. removing from said converted  $C$  the quantity that  $d_{sub.i}$  introduced (column 9 lines 17-22).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Kurumatani discloses:

A cryptographic system as in claim 18, where said encryption is carried out, in lieu, independently on self-contained components, comprising:

means for calculating  $c$  by carrying out two or more of said additions (+) and/or by computing two or more of said terms  $d_{sub.i}z_{sub.ij}$  and  $f_{sub.i}(d_{sub.i})v_{sub.ij}$  in parallel (column 9 lines 14-17).

Claim 20 is rejected as applied above in rejecting claim 15. Furthermore, Kurumatani discloses:

A cryptographic system, as in claim 15, for communicating a message securely from a first party E to a second party D comprising:

means for obtaining at party D arbitrary and/or random input from which cryptographic keys are generated (column 5 lines 53-61);

means for generating at party D a decryption key to be kept secret (column 8 lines 39-64);

means for generating at party D one of a plurality of corresponding encryption keys (column 9 lines 1-22);

means for distributing said encryption key from party D to party E (column 9 lines 14-17);

means for accepting a message  $m$  at party E (column 9 lines 14-17);

means for encrypting  $m$  to ciphertext at party E, employing encryption key (column 9 lines 14-17);

means for transmitting said ciphertext from party E to party D (column 9 lines 14-22);

means for receiving said ciphertext at party D (column 9 lines 14-22); and

means for decrypting said ciphertext at party D to recover m, employing said decryption key (column 9 lines 17-22).

### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA  
6/23/05

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100